AN OVERVIEW OF AUTOMATED PENETRATION TESTING

Kiranben Chaudhari, Seema Joshi
Student, GTU- School of Engineering and Technology
Assistant Professor, Gujarat Technological University

Abstract: With increasing internet connectivity all over the world. The accessibility for the data resources also increases so the threats to the integrity, confidentiality and availability of data also increase. As the result of this the different attack like hacking exploitation also increases. To perform this attack or to prevent from this kinds of attack the organization are performing vulnerability assessment and penetration testing on a regular basis but Vulnerability assessment can be perform using tools available where as penetration testing is done manually by using logics. So we would make tool which will cut down problem of doing Penetration testing manually. Limitation of manual testing is it depends upon the individual& skill. This automated tool will search all the vulnerabilities as well as perform exploitation automatically. This would save time as well as increase the efficiency of work.

Index Terms—Vulnerability Assessment, Penetration testing, OWASP-ZAP

I. INTRODUCTION

Web application usage has increased as more and more services are available on the web. A business using Web applications is also increasing day by day. On the other side, a web application based attacks have increased. The web application has become the main target of attackers. The Major impact of attacks is a data loss or financial loss or reputation loss.

Various types of countermeasures exist to protect system against attacks like defensive coding, firewall, Intrusion detection system etc. [1]. The existing solutions are classified in two categories proactive and reactive. To secure web applications, thorough study of vulnerabilities is required. The study will help in taking effective actions. Vulnerability measurement and Penetration testing are widely used approaches by organizations for web application security assessment.

Vulnerability is a weakness or flaw in a system. Reasons for vulnerability existence are weak password, coding, input validation, Misconfiguration etc. The attacker attempts to identify vulnerabilities and then work it. Vulnerability assessment is a proactive and systematic strategy to discover vulnerability. It is practiced to discover unknown problems in the system. Vulnerability assessment is achieved using scanners. It is a hybrid solution, which combines automated testing with expert analysis.

Penetration testing is used to check the exploitations and the vulnerability of the organization's system and help the developers to build a protected system that meets the needs. It's very important to any organization and company to protect their data and information from outside attackers and keep monitoring to the prioritize the severity of the security issues. Determining the priorities can help the developers to determine the needed devices in the allocation of the budget for security issues. Additionally, can be used to find the financial loss expected and risks if the attackers achieve their goals and exploited the system and how to mitigate that. The data generated from the test considered confidential and private data because it shows approximately all the holes in the system and how they could be exploited. [2]

PT can be done by attacking the system similar to the action of the outside attackers and find out what can be obtained [3]. The attack might not be as easy as exploiting one vulnerability, many vulnerabilities may be used to achieve the goal by making a sequence of attack chain (Multi-step attack) [4]. It's also considered as a risk assessment and can be used to check the network safety. When penetration test is done, the roles of engagement for that test should be set also, to set the goals and the methodology of the test.

Penetration tests companies can be classified into three different types: gray hat, black hat, and white hat. In the white hat, the tester is an ethical hacker that respects the rules of the organization and the employees can help to perform the testing. While the black hat is mainly used to find how the employees interact with the undesired attack, in this approach the administrators are only the ones who know the test is underway. Moreover, we can do a Gray hat which is a combined approach to the previous types into a custom test plan [5].

II. PHASES OF PENETRATION TESTING

There is no hard and fast rule of conducting penetration testing with respect to phases of conducting penetration test however common phases that every tester must have to go through are 1. Reconnaissance, 2. Execution, 3. Discovery. These three steps are baseline of each penetration test however these phases are further divided into sub phases for convenience of penetration testers. I recommend seven phases of a professional penetration testing on a target network.

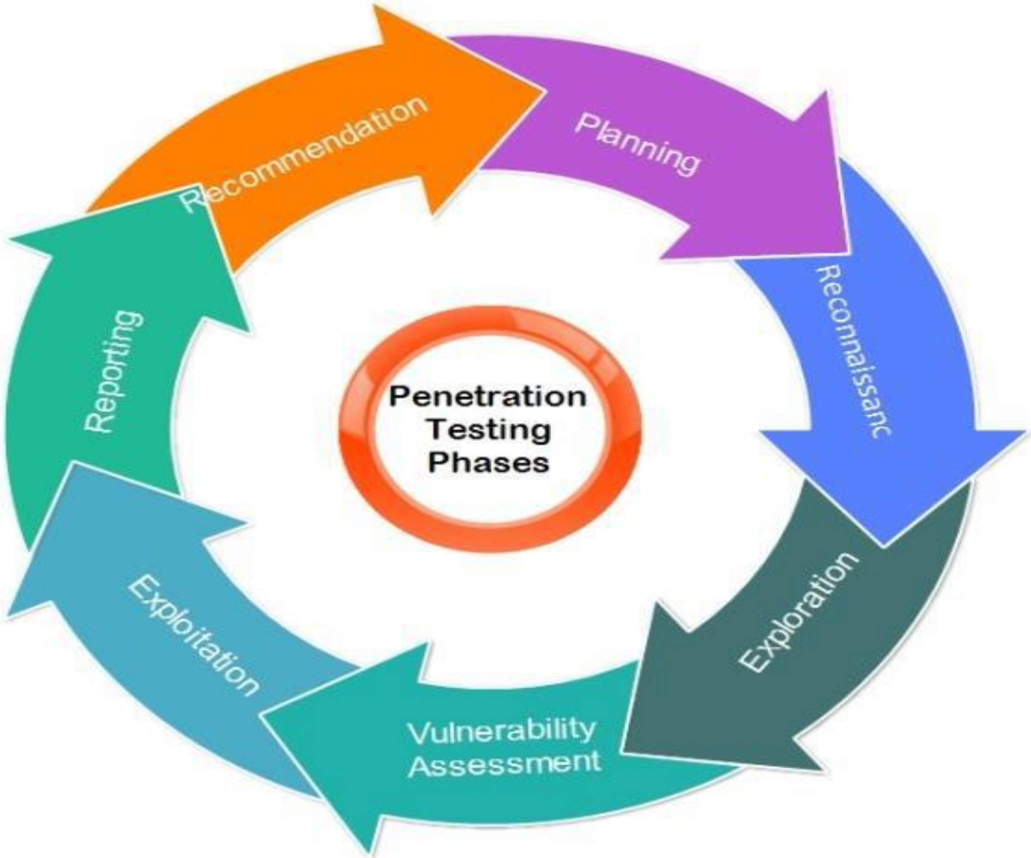


Fig: Phases of Penetration Testing [6]

Planning: In Planning phase scope of the test is determined, Like in which system test is to be done , how it should be done and who will perform this test , what will be the time frame, what should be the benefit to the organization , all these things are checked in planning phase of Pen-testing

Reconnaissance: After the scope of the test is done, this is the second phase in which Information gathering about target network. Information as much as possible are gathered in this phase. This is a complete phase which may consist of identifying target network status, operating systems, IP addresses range, open ports, domain name, DNS, DHCP, Wifi Key, Mail Server Records etc. Host Finger Printing, Port Scanning, Network Mapping, Network Enumeration are usually considered in reconnaissance phase.

Exploration: This is the third phase that deals with exploring the entire network based on necessary information gathered in reconnaissance phase. More precise to the network services. Like checked opened ports in last step. Using opened ports, the tester enters the network and explore the network more deeply. Testers scans the network for discovering network devices, firewall rules, users accounts and access control etc.

Exploration include host exploration, services identification and platform identification etc.

Vulnerability Assessment: Vulnerability is a path through which threats are revealed. Vulnerabilities are actually weakness in the system. Vulnerability assessment is the process of computing, ranking and pinpointing the vulnerabilities in the system. Penetration testers may use automated tools for known vulnerabilities. These tools are helpful by having updated databases for latest vulnerabilities and their details.

Exploitation: This is most difficult phase in penetration testing which deals with attacks to the target network. The penetration tester tries to exploits for different vulnerabilities discovered in last phase. Privilege Escalation in considered sub part of exploitation phase in which usually attacker takes advantage of programming bugs or design loopholes to crawl to the privileged access that are usually protected general users and applications. The system having more privileged accounts can be exploits up to more extent.

Reporting and Recommendation: This last phase in which documentation is done by testing team. This is final document on which all the phases based. The main object of penetration test is to point out all flaws and weakness in a network or a system that have covered in last phases. Final report should cover all phases' activities including a cover sheet, executive summary of vulnerabilities found in the network, threats imposed from these vulnerabilities, list of tools used and most important final recommendation after overall examination of test report. Upon final recommendation covered in the report, values of threats and mitigation of threats are discussed. Final recommendation phase must be done with upper level management in which preventive proposals are provided against founded vulnerabilities.

III. PENETRATION TESTING STANDARDS

Following is the list of professional standards and certifications regarding penetration testing. These organizations are well known and are accredited throughout the Information Security World.

o EC-Council LPT (Licensed Penetration Tester)

o OSTTMM(Open Source Security Testing Methodology Manual)

o PTF (Penetration Testing Framework)

o OWASP(Open Web Application Security Project)

o ISSAF (Information Systems Security Assessment Framework)

o WASC-TC(Web Application Security Consortium Threat Classification)

o OISSG (Information Systems Security Assessment Framework)

o PCI DSS v3.1 (Payment Card Industry Data Security Standard)

o ISO/IEC27001:2005(Information Security Management Systems)

o ISO/IEC 27005:2008 (Information Security Risk Management)

IV. MANUAL VS. AUTOMATED PENETRATION TESTING

Until recently, Penetration testing has been restricted to advanced security specialist that having many years of relevant experience to do the complex manual process. but in fact, the proficient penetration testers are not highly available and the manual process is time and money consuming. A team of experts can gather to build a professional automated tool that can be a combination of experience of the expert penetration testers. so that the non-expert users can substitute the penetration team with the automated tools to get an inclusive view of the security situation on the organization's system.

The table below, summaries the comparison between manual and automated penetration testing:

Table 1: Comparison of manual and automated testing[7] [8]

	Automated Penetration testing	Manual Penetration testing
Testing process	Fast, standard process; Easily repeatable tests	Manual, non-standard process; capital intensive; High cost of customization
Vulnerability /attack Database management	Attack database is maintained and updated attack codes are written for a variety of platforms	Maintenance of database is manual; Need o rely on public

		database; Need re-write attack code for functioning across different platforms
Exploit Development and Management	Product vendor develops and maintains all exploits. Exploits are continually updated for maximum effectiveness. Exploits are professionally developed, thoroughly tested, and safe to run. Exploits are written and optimized for a variety of platforms and attack vectors	Developing and maintaining an exploit database is time consuming and requires significant expertise. Public exploits are suspect and can be unsafe to run. Re-writing and porting code is necessary for cross platform functionality.
Reporting	Reports are automated and customized	Requires collecting the data manually
Cleanup	Automated testing products offer clean-u solutions	The tester has to manually undo the changes to the system every time vulnerabilities found
Auditing	Automatically records a detailed record of all activity.	Slow, cumbersome, often inaccurate process
Training	Training for automated tools is easier than manual testing	Testers need to learn nonstandard ways of testing ; training can be customized and is time consuming

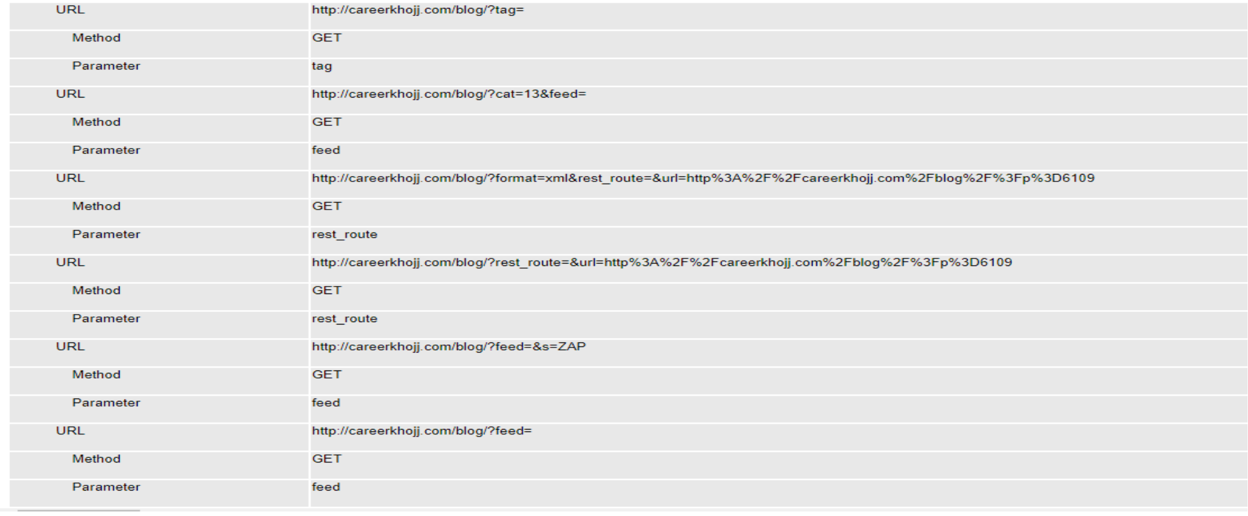
V. EXISTING TOOL

Tool: OWASP -ZAP (Zed Proxy Attack[9]

Feature: Automated Penetration testing tool , Intercepting proxy, Active & passive scanner, Spider, Brute force, Port scanner, Session comparison, Parameter analysis.[12]

Portability: Window, Linux and MacOS

Automated Sql injection detect in OWASP-ZAP



URL	http://careerkhojj.com/blog/?tag=
Method	GET
Parameter	tag
URL	http://careerkhojj.com/blog/?cat=13&feed=
Method	GET
Parameter	feed
URL	http://careerkhojj.com/blog/?format=xml&rest_route=&url=http%3A%2F%2Fcareerkhojj.com%2Fblog%2F%3Fp%3D6109
Method	GET
Parameter	rest_route
URL	http://careerkhojj.com/blog/?rest_route=&url=http%3A%2F%2Fcareerkhojj.com%2Fblog%2F%3Fp%3D6109
Method	GET
Parameter	rest_route
URL	http://careerkhojj.com/blog/?feed=&s=ZAP
Method	GET
Parameter	feed
URL	http://careerkhojj.com/blog/?feed=
Method	GET
Parameter	feed

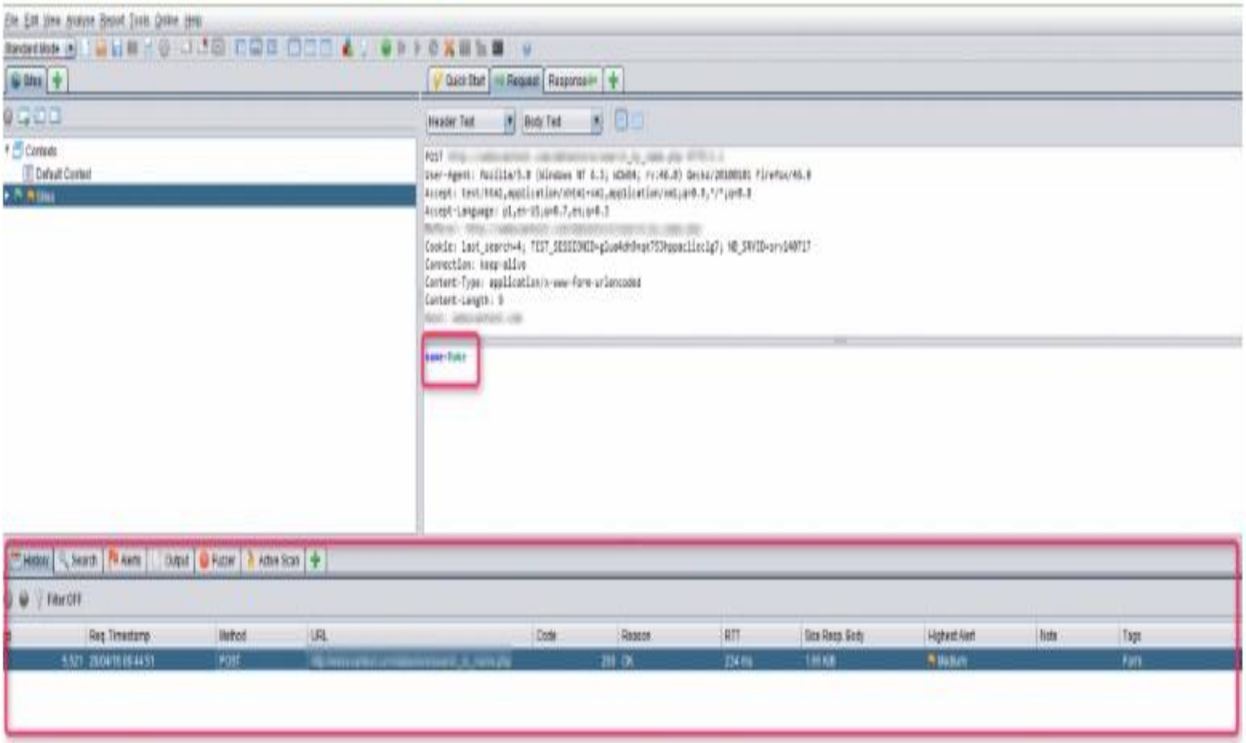
Figure :Result Analysis 1

Manually Sql injection Exploit in OWASP-ZAP

1.In application, find the field where you can send the POST request.

2.After sending the POST request in web application, go back to OWASP ZAP.

3.In the History tab, you will see your POST request and, above it, the value which has been entered in the POST request; in this case 'name=Rake'.

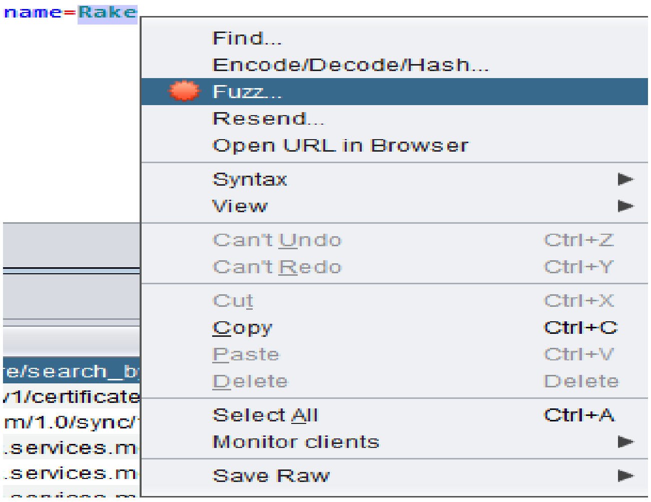


```
POST [illegible]
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: pl,en-US;q=0.7,en;q=0.3
Referer: [illegible]
Cookie: last_search=4; TEST_SESSIONID=g1ue4dh9npk753hppacllec1g7; HD_SRVID=srv140717
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 9
Host: [illegible]

name=Rake
```

	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags
5,521	20/04/18 05:44:51	POST	[illegible]	200	OK	234 ms	1.95 KiB	Medium		Form

Figure: process of manual testing in sql injection

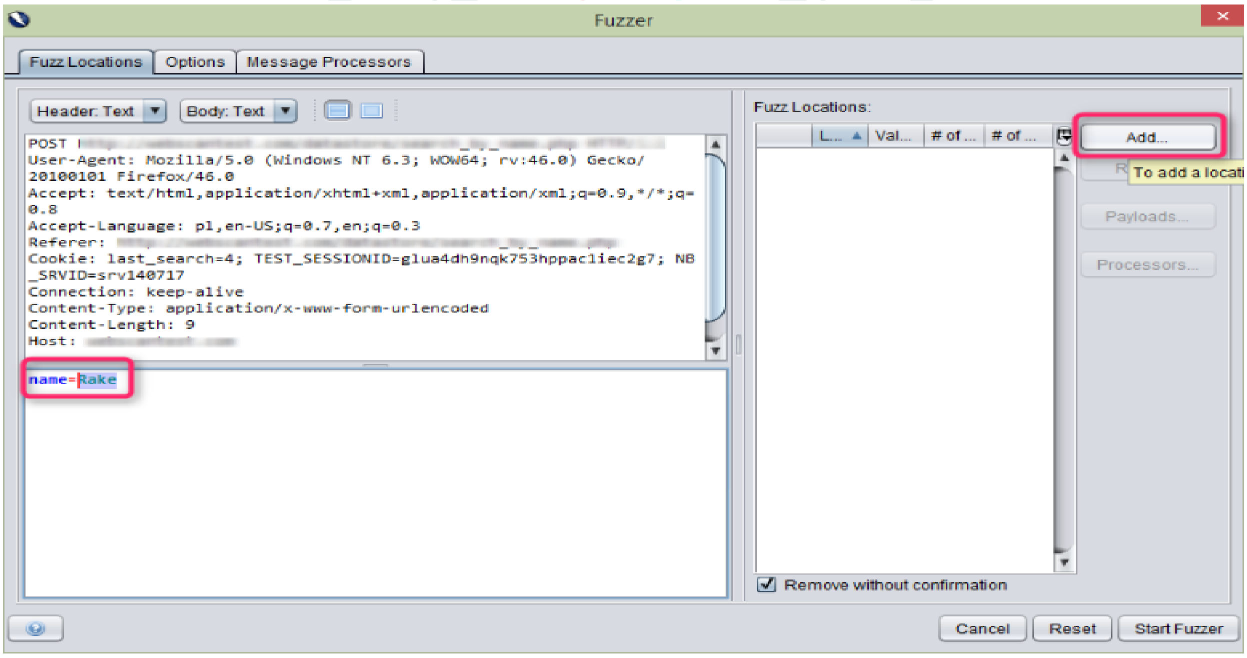
4.Mark the content 'Rake', Right-click on it and click 'Fuzz…'.



```
name=Rake
```

Figure : process of manual testing in sql injection

5.A new window will be displayed. Again, mark 'Rake' and click 'Add…



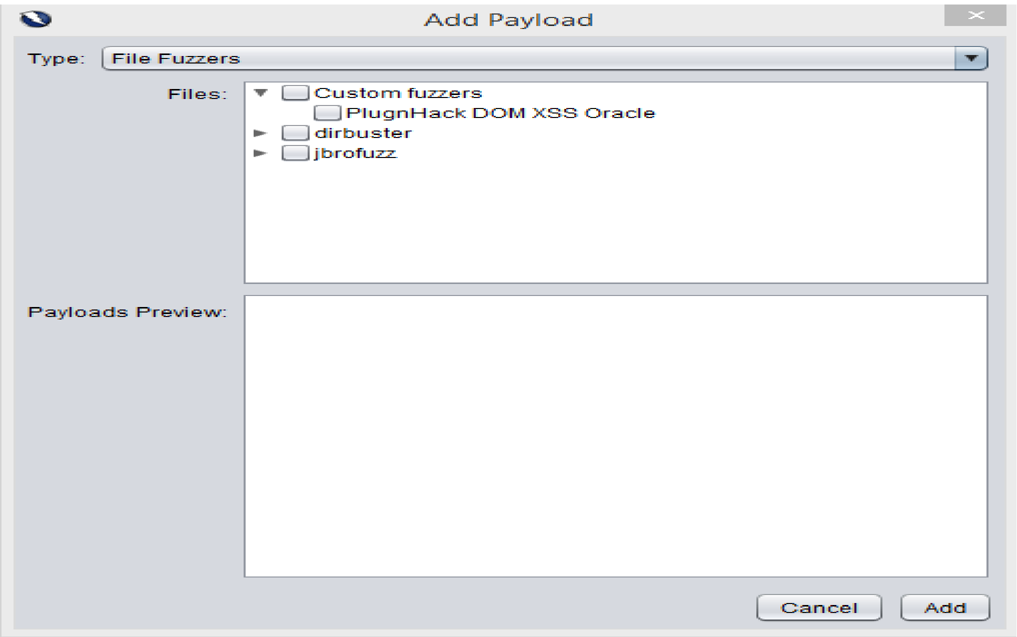
```
POST [redacted]
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:46.0) Gecko/
20100101 Firefox/46.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=
0.8
Accept-Language: pl,en-US;q=0.7,en;q=0.3
Referer: [redacted]
Cookie: last_search=4; TEST_SESSIONID=glua4dh9nqk753hppac1iec2g7; NB
_SRVID=srv140717
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 9
Host: [redacted]

name=Rake
```

☑ Remove without confirmation

Figure : process of manual testing in sql injection

6. The 'Payloads' window will be displayed, in which you need to click the 'Add…' button again

7. Choose ‘File Fuzzers’ from the ‘Type:’ dropdown in the ‘Add payload’ window.



Add Payload

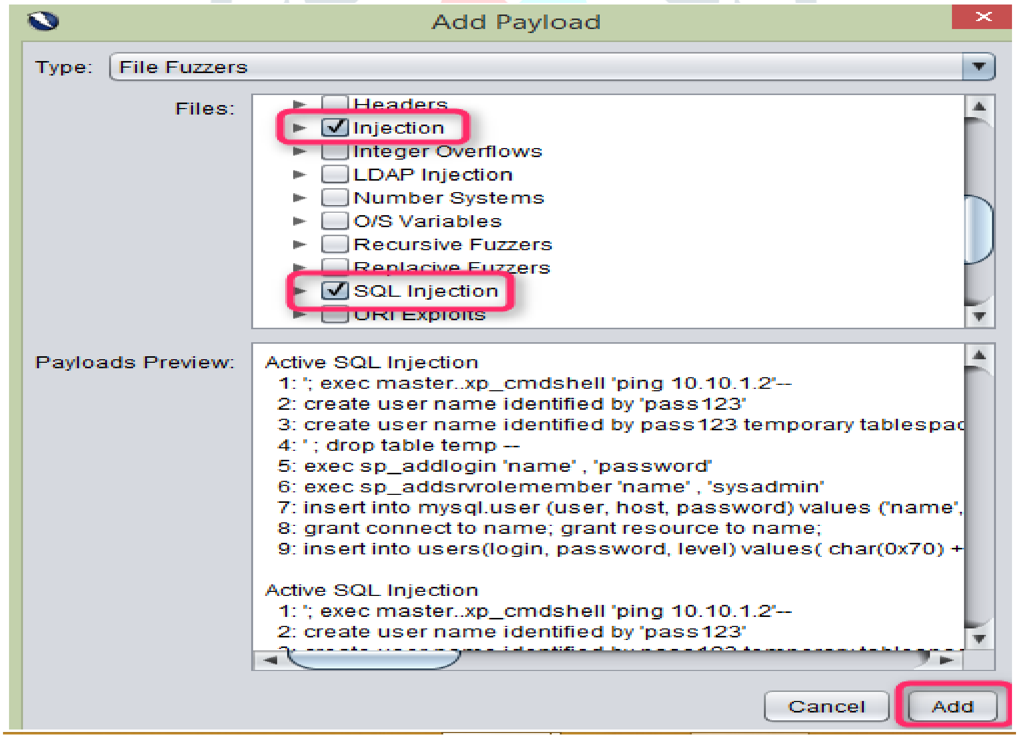
Type: File Fuzzers

Files:
- □ Custom fuzzers
  - □ PlugnHack DOM XSS Oracle
- □ dirbuster
- □ jbrofuzz

Payloads Preview:

Figure : process of manual testing in sql injection

8. Expand the ‘jbrofuzz’ list and mark the two checkboxes labelled ‘Injection’ and ‘SQL Injection’ from the expanded list. Click on the ‘Add’ button.



Add Payload

Type: File Fuzzers

Files:
- □ Headers
- ☑ Injection
- □ Integer Overflows
- □ LDAP Injection
- □ Number Systems
- □ O/S Variables
- □ Recursive Fuzzers
- □ Replacive Fuzzers
- ☑ SQL Injection
- □ URI Exploits

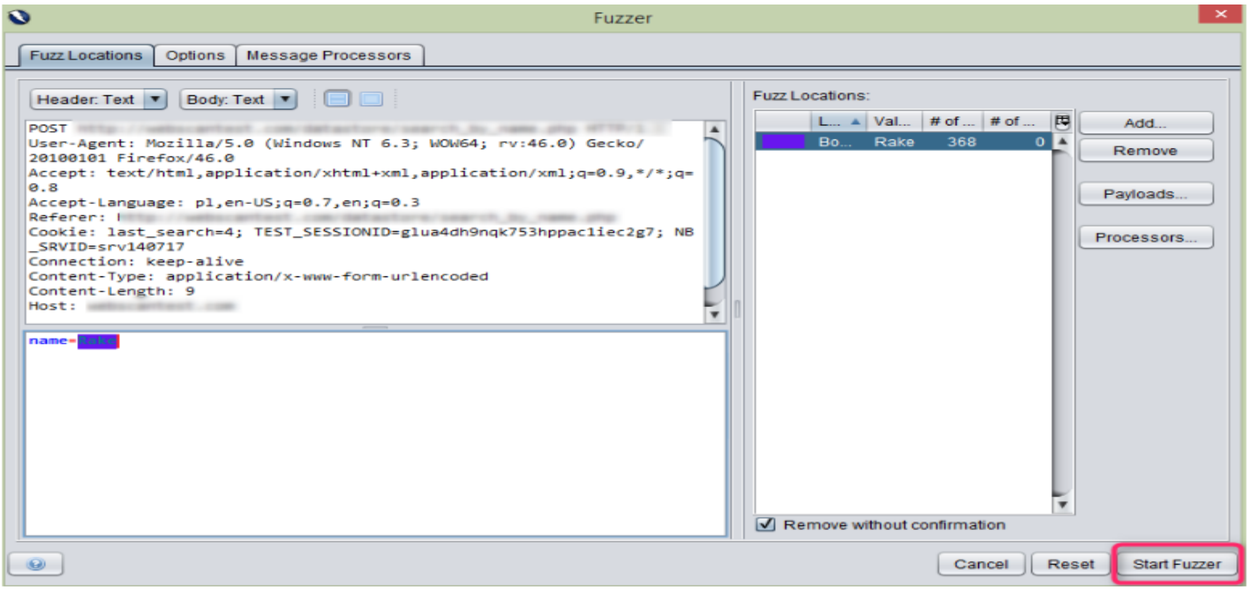
Payloads Preview:

```
Active SQL Injection
  1: '; exec master..xp_cmdshell 'ping 10.10.1.2'--
  2: create user name identified by 'pass123'
  3: create user name identified by pass123 temporary tablespac
  4: ' ; drop table temp --
  5: exec sp_addlogin 'name' , 'password'
  6: exec sp_addsrvrolemember 'name' , 'sysadmin'
  7: insert into mysql.user (user, host, password) values ('name',
  8: grant connect to name; grant resource to name;
  9: insert into users(login, password, level) values( char(0x70) +

Active SQL Injection
  1: '; exec master..xp_cmdshell 'ping 10.10.1.2'--
  2: create user name identified by 'pass123'
```

Figure : process of manual testing in sql injection

9. In the ‘Payloads’ window click the “OK” button.

10. In the 'Fuzzer' window click the 'Start Fuzzer' button.



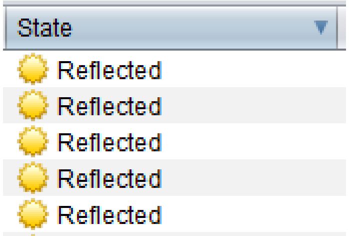
```
POST [redacted]
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:46.0) Gecko/
20100101 Firefox/46.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=
0.8
Accept-Language: pl,en-US;q=0.7,en;q=0.3
Referer: [redacted]
Cookie: last_search=4; TEST_SESSIONID=glua4dh9nqk753hppac1iec2g7; NB
_SRVID=srv140717
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 9
Host: [redacted]

name=Rake
```

L... ▲	Val...	# of ...	# of ...
Bo...	Rake	368	0

☑ Remove without confirmation

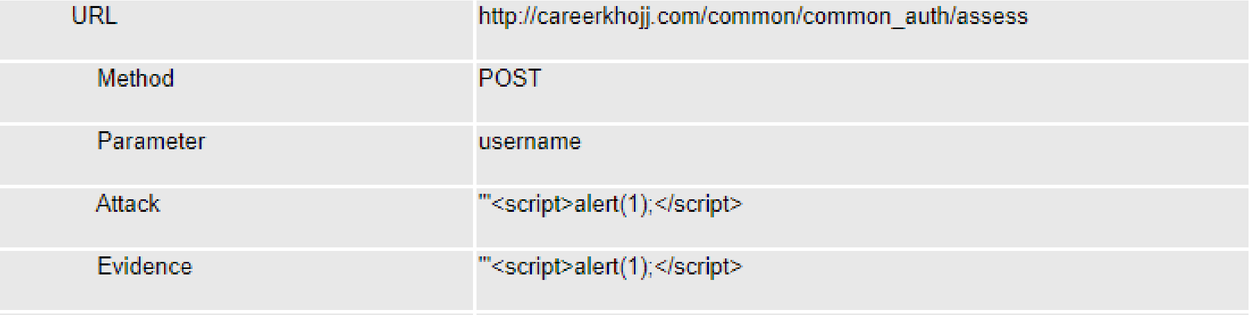
Figure : process of manual testing in sql injection

11. In the 'Fuzzer' tab, you can see that the field, in which the POST request has been executed, is now being attacked by dozens of SQL requests that may be potentially dangerous for your application. Requests with the 'Reflected' status in the 'State' column are safe for the application – the rest, however, may be not.



State
Reflected
Reflected
Reflected
Reflected
Reflected

Automated Cross site scripting detect and exploit in OWASP-ZAP



URL	http://careerkhojj.com/common/common_auth/assess
Method	POST
Parameter	username
Attack	'"<script>alert(1);</script>
Evidence	'"<script>alert(1);</script>

Figure : Resu1t Analysis 2

VI. CONCLUSION AND FUTURE WORK

Many organizations need penetration testing to discover the most vulnerabilities that have in their system. To apply the penetration test, there are two approaches that the organizations used to discover the bugs, one is automated penetration test and the other is manual penetration test. The automated pen test is the easiest way to figure out the whole vulnerabilities in the system by implementing a tool that has some patterns to find the vulnerabilities. While the manual test is the way to discover the vulnerabilities manually through analyzing the system and distinguish the abnormal behavior.

Hence, this paper has been done to shows the importance of the penetration testing as well as the importance of automating this process . Additionally, some standards in the penetration testing have been highlighted to help the researchers find the suitable standards to use. Even more, the comparison between the manual and automated penetration testing has been provided in term of the testing process, vulnerability and attack database management, exploit development and management reporting, clean up, logging, and training. And the result shows that the automated penetration testing is better than the manual penetration in all of the above process, except finding the new or zero day exploits. So that many organizations may go for the automated approach because it seems the better and cheaper way to maintain security in the systems as most of the vulnerabilities that the attackers used to exploit the system are well defined in the automated tools. Although writing own exploits may be time-consuming as well as ineffective in terms of money. But, the attackers can conceal their activity through their own scripts. Thus, the automated tools still have limitations and vulnerabilities.

To the best of our knowledge, this research is a step forward to the other researchers who interested in the automated penetration testing. The next step is to study the impact of the penetration testing toward the hunting threats. Even more, to study the applicability of building automated tool that takes into consideration the general limitations in the current automated tools.

VII. REFERENCE

[1] Jignesh Doshi, Bhushan Trivedi, Assessment of SQL Injection Solution Approaches, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 10, October 2014 ISSN: 2277 128X

[2] Y. Stefinko, A. Piskozub and R. Banakh, "Manual and automated penetration testing. Benefits and drawbacks. Modern tendency," 2016 13th International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET), Lviv, 2016, pp. 488-491. doi: 10.1109/TCSET.2016.7452095

[3] Xue Qiu, Shuguang Wang, Qiong Jia, Chunhe Xia and Qingxin Xia, "An automated method of penetration testing," 2014 IEEE Computers, Communications and IT Applications Conference, Beijing, 2014, pp. 211-216.
doi: 10.1109/ComComAp.2014.7017198

[4] L. Greenwald and R. Shanley, "Automated planning for remote penetration testing," MILCOM 2009 -2009 IEEE Military Communications Conference, Boston, MA, 2009, pp. 1-7.
doi: 10.1109/MILCOM.2009.5379852

[5] Gula, Ron. “Broadening the Scope of Penetration Testing Techniques.” Jul. 1999. URL: www.forumintrusion.

[6] Knowles, W., Baron, A., & McGarr, T. (2015). Analysis and recommendations for standardisation in penetration testing and vulnerability assessment: penetration testing market survey.

[7] Y. Stefinko, A. Piskozub and R. Banakh, "Manual and automated penetration testing. Benefits and drawbacks. Modern tendency," 2016 13th International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET), Lviv, 2016, pp. 488-491. doi: 10.1109/TCSET.2016.7452095U.

[8] Mirjalili, Mahin, Alireza Nowroozi, and Mitra Alidoosti. "A survey on web penetration test." International Journal in Advances in Computer Science 3.6 (2014).

[9] https://en.wikipedia.org/wiki/OWASP_ZAP

[10] Open Web Application Security Project, https://www.owasp.org/index.php/Category: Vulnerability

[11] Goel, J. N., & Mehtre, B. M. (2015). Vulnerability assessment & penetration testing as a cyber defence technology. *Procedia Computer Science*, *57*, 710-715.

[12] Hai Zhou LING “towards the automation of vulnerability detection in source code” Master of Computer Science, Concordia University, Montréal, Québec, Canada

[13] Jeremiah Grossman WhiteHat Security founder & CTO “Website Vulnerabilities Revealed “ WhiteHat Security

[14] Stefan Kals, Engin Kirda, Christopher Kruegel, and Nenad “ SecuBat: A Web Vulnerability Scanner” Stefan Kals, Engin Kirda, Christopher Kruegel, and Nenad Jovanovic Secure Systems Lab, Technical University of Vienna

[15] Daisy Suman, Sarabjit Kaur and Geetika Mannan, “Penetration Testing”, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 10, October 2014.